UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

ERIC KIRKHAM, derivatively on behalf of HEARTLAND PAYMENT SYSTEMS, INC. Plaintiff, v. ROBERT O. CARR, MITCHELL L. HOLLIN, ROBERT H. NIEHAUS, MARC J. OSTRO, JONATHAN J. PALMER, GEORGE F. RAYMOND, RICHARD W. VAGUE, and ROBERT H.B. BALDWIN, JR. Defendants, and HEARTLAND PAYMENT SYSTEMS, INC., Nominal Defendant.	Civil Action No. **JURY TRIAL DEMANDED**

VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT

1. Plaintiff Eric Kirkham ("Plaintiff"), by and through his undersigned attorneys, hereby submits this Verified Shareholder Derivative Complaint (the "Complaint") for the benefit of nominal defendant Heartland Payment Systems, Inc. ("Heartland" or the "Company") against certain current and former members of its Board of Directors (the "Board") and executive officers seeking to remedy defendants' breaches of fiduciary duties and unjust enrichment from February 2008 to the present (the "Relevant Period").

NATURE OF THE ACTION

2. According to its public filings, Heartland provides bank card payment processing services to more than 250,000 merchants and businesses worldwide. The Company's services

involve facilitating the exchange of information and funds between merchants and cardholders' financial institutions; and providing end-to-end electronic payment processing services to merchants, including merchant set-up and training, transaction authorization and electronic draft capture, clearing and settlement, merchant accounting, merchant assistance and support, and risk management. The Company also offers payroll processing, gift and loyalty programs, and paper check processing services, as well as sells and rents point-of-sale devices and supplies.

3. Beginning in February 2008, defendants caused Heartland to issue a series of materially false and misleading statements concerning the Company's business operations and financial condition and caused Heartland to file a series of materially false and misleading statements with the U.S. Securities and Exchange Commission (the "SEC").

4. On January 20, 2009, however, defendants revealed for the first time that Heartland's payment processing network had been breached within its processing system by malicious so-called "sniffer software" or "malware" that had been capturing, among other things, debit card numbers, expiration dates, and cardholder names. This security breach potentially exposed tens of millions (if not more) of debit card holders to fraud.

5. On this news, shares of Heartland common stock fell by $1.26 per share, or over 8%, to close on January 20, 2009 at $14.18 per share on unusually heavy volume.

6. On January 22, 2009, *Bloomberg* published an article about the security breach at Heartland. The *Bloomberg* article stated that the security breach may have involved up to 100 million accounts, which would be double the size of the largest such breach in history.

7. Upon the release of this news, the Company's shares declined by $5.93 per share, or more than ***42%***, to close on January 22, 2009 at $8.18 per share, on unusually heavy trading volume.

8. Then, on February 24, 2009, defendants caused the Company to announce disappointing quarterly financial results in an earnings press release. Additionally, defendants caused the Company to announce that it was cutting its stock dividend by 72%, and further warned that Heartland could face losses due to the security breach.

9. Later that day, during an earnings conference call, defendants disclosed that the Company was under investigation by the SEC, the U.S. Department of Justice (the "DOJ"), the U.S. Federal Trade Commission (the "FTC"), and the Office of the Comptroller of the Currency (the "Comptroller").

10. Upon the release of this news, the Company's shares fell an additional $2.31 per share, or more than ***30%***, to close on February 24, 2009 at $5.34 per share, also on unusually heavy trading volume.

11. Throughout the Relevant Period, defendants failed to disclose: (1) that the Company was in imminent danger of having the security of its processing system breached; (2) that defendants had not taken the proper steps to secure the Company's systems; (3) that it was likely that the Company would not be aware that such a breach had occurred until weeks or months after the fact; (4) that defendants had been notified of a potential breach in the Company's security system; (5) that the Company's payment processing system had been infected as early as May 2008 with malware; (6) that as a result, the Company would face significant costs related to, among other things, liability and the implementation of proper measures; and (7) that the Company lacked adequate internal controls.

12. Defendants' misconduct has significantly harmed this once valuable Company, causing Heartland's stock price to plummet and subjecting the Company to substantial costs associated with multiple governmental investigations, and potential liability for violation of

numerous state and federal laws.

JURISDICTION AND VENUE

13. This Court has jurisdiction over all causes of action asserted herein pursuant to 28 U.S.C. §1332(a)(2) in that Plaintiff and defendants are citizens of different states and the matter in controversy exceeds $75,000, exclusive of interest and costs.

14. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District, or is an individual who has sufficient minimum contacts with New Jersey so as to render the exercise of jurisdiction by this District permissible under traditional notions of fair play and substantial justice.

15. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a) because one or more of the defendants either resides in or maintains executive offices in this District, a substantial portions of the transactions and wrongs complained of herein, including the defendants' primary participation in the wrongful acts detailed herein in violation of their fiduciary duties owed to Heartland occurred in this District, and defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

THE PARTIES

16. Plaintiff is a current shareholder of Heartland and has continuously held Heartland stock since September 7, 2007. Plaintiff is a citizen of North Carolina.

17. Nominal defendant Heartland is a Delaware corporation that maintains its corporate headquarters at 90 Nassau Street, Princeton, New Jersey 08542.

18. Defendant Robert O. Carr ("Carr") has served as Heartland's Chief Executive

Officer ("CEO") and Chairman of the Board since 2000. Upon information and belief, defendant Carr is a citizen of New Jersey.

19. Defendant Mitchell L. Hollin ("Hollin") has served as a director of the Company since October 2001. Upon information and belief, defendant Hollin is a citizen of Pennsylvania.

20. Defendant Robert H. Niehaus ("Niehaus") has served as a director of the Company since October 2001. Upon information and belief, defendant Niehaus is a citizen of New York.

21. Defendant Jonathan J. Palmer ("Palmer") has served as a director of the Company since November 2003. In addition, defendant Palmer has served as a member of the Board's Audit Committee (the "Audit Committee") during the Relevant Period. Upon information and belief, defendant Palmer is a citizen of Texas.

22. Defendant George F. Raymond ("Raymond") has served as a director of the Company since March 2004. In addition, defendant Raymond has served as a member of the Audit Committee during the Relevant Period. Upon information and belief, defendant Raymond is a citizen of Florida.

23. Defendant Marc J. Ostro ("Ostro") has served as a director of the Company since October 2002. In addition, defendant Ostro has served as a member of the Audit Committee during the Relevant Period. Upon information and belief, defendant Ostro is a citizen of Pennsylvania.

24. Defendant Richard W. Vague ("Vague") has served as a director of the Company since May 2007. Upon information and belief, defendant Vague is a citizen of Pennsylvania.

25. Defendant Robert H.B. Baldwin ("Baldwin") has served as President and Chief Financial Officer ("CFO") of the Company since 2000. Upon information and belief, defendant

Baldwin is a citizen of New Jersey.

26. Collectively, defendants Carr, Hollin, Niehaus, Palmer, Raymond, Ostro, Vague, and Baldwin shall be referred to herein as "Defendants."

27. Collectively, defendants Palmer, Raymond, and Ostro shall be referred to as the "Audit Committee Defendants."

DEFENDANTS' DUTIES

28. By reason of their positions as officers, directors, and/or fiduciaries of Heartland and because of their ability to control the business and corporate affairs of Heartland, Defendants owed Heartland and its shareholders fiduciary obligations of good faith, loyalty, and candor, and were and are required to use their utmost ability to control and manage Heartland in a fair, just, honest, and equitable manner. Defendants were and are required to act in furtherance of the best interests of Heartland and its shareholders so as to benefit all shareholders equally and not in furtherance of their personal interest or benefit. Each director and officer of the Company owes to Heartland and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

29. Defendants, because of their positions of control and authority as directors and/or officers of Heartland, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein. Because of their advisory, executive, managerial, and directorial positions with Heartland, each of the Defendants had knowledge of material non-public information regarding the Company.

30. To discharge their duties, the officers and directors of Heartland were required to exercise reasonable and prudent supervision over the management, policies, practices and

controls of the Company. By virtue of such duties, the officers and directors of Heartland were required to, among other things:

a. Exercise good faith to ensure that the affairs of the Company were conducted in an efficient, business-like manner so as to make it possible to provide the highest quality performance of their business;

b. Exercise good faith to ensure that the Company was operated in a diligent, honest and prudent manner and complied with all applicable federal and state laws, rules, regulations and requirements, and all contractual obligations, including acting only within the scope of its legal authority; and

c. When put on notice of problems with the Company's business practices and operations, exercise good faith in taking appropriate action to correct the misconduct and prevent its recurrence.

31. Pursuant to the Audit Committee's Charter, the purpose of the Audit Committee is to act on behalf of the Board in monitoring, among other things: (1) the integrity of the Company's financial statements and the Company's financial reporting and disclosure practices; (2) the compliance by the Company with ethical policies and legal and regulatory requirements; and (3) the Company's internal controls.

32. Pursuant to the Audit Committee Charter, the Audit Committee Defendants were and are required, *inter alia*, to:

a. Discuss earnings press releases and financial information with management;

b. Review with management, in connection with the Company's annual and quarterly financial statements prior to their filing with the SEC, the adequacy of the Company's internal controls;

c. Meet with management to review the Company's major financial risk exposures and the steps management has taken to monitor and control such exposures;

d. Advise the Board with respect to the Company's policies and procedures regarding compliance with applicable laws and regulations and with the Company's Code of Business Conduct and Ethics;

e. Discuss with management any significant legal, compliance or regulatory

matters that may have a material effect on the financial statements or the Company's business, including inquiries received from governmental agencies; and

f. Monitor the Company's financial reporting process and systems of internal controls.

33. Heartland's Code of Business Conduct and Ethics for Directors, Officers, and Employees provides, among other things, that the Company's directors and senior officers "are committed to providing our stockholders and investors with full, fair, accurate, timely, and understandable disclosure in the reports that we file with the Securities and Exchange Commission."

SUBSTANTIVE ALLEGATIONS

34. On February 13, 2008, Defendants caused the Company to hold an earnings conference call with investors and financial analysts. During the call, defendants Baldwin and Carr stated, in pertinent part:

> [Baldwin]: Remember we accrued the buyout liability based on margin generated by existing merchants and with December's weakness this accrual came in low. G&A expenses rose 37% this quarter much higher than the more moderate growth we consistently achieved over the last few years. The increases were primarily driven by IT expenditures required to bolster our internal security and disaster recovery capabilities. In addition as Bob mentioned we had a host of what I call onetimers in everything from legal to marketing this quarter.
>
> * * *
>
> [Participant]: Bob, I wanted to ask you about the security spend you talked about or the IT spend. Was there a particular reason – I mean was there a necessity for this? Did you see the particular flaw that may do you do this or was this just as a result of somebody else taking over and they felt there was a need for a spend?
>
> [Carr]: We were surprised frankly with some of the inadequacies in our disaster recovery in our business continuity model. We have moved to a data warehousing approach and just in the process of doing our planning for '08 we discovered a couple of things we felt made us more vulnerable than we wanted to be and we decided to take -- go ahead and bite the bullet and do what we thought was the right thing and spend the money in the fourth quarter. So that we felt we could in good conscience say that we have a very very secure system and as much to the extent that we know how to make it secure. So it was a surprise, it was a negative surprise that came as a result of us getting new information about some of what we had developed in the past.

* * *

[Analyst]: I was hoping we could go back into the disaster recovery investment. Can you just I guess tell us a little bit more about what prompted the review of the disaster recovery? Was there a specific incident or was it a proactive review that triggered that thinking?

[Carr]: There were a couple of things that we learned as we reassigned responsibilities. We learned that there was -- there were some significant vulnerabilities that thank goodness we didn't suffer any results from those vulnerabilities but we could have.

And I think this is true of a lot of IT shops frankly sometimes it's good to have new blood come in and take a look at the firewalls that are developed and the internal controls of the existing people. And we just found that the veteran team had gotten comfortable with the systems they set up years ago and they weren't effective anymore. And so it's a combination of a number of things. We also decided to kill a contract for a datacenter that we were going to set up in the Southeast and we're keeping all that in Texas. And that's caused us to have to do a write-off of a space that we never occupied and we think for the long-term we made the right decision there as well.

[Analyst]: Just to be clear there was never any action? It was just a fresh look at it through some new personnel and you were able to identify an area that should have been highlighted?

[Carr]: I wouldn't say it's new personnel. It's new facts that became evident to senior management about some of the weaknesses in the firewalls and in the internal controls of our people.

[Analyst]: Was there any particular incident that triggered that? That's what I'm trying to get at is this something (multiple speakers)

[Carr]: The incident was that new people came in and looked at our systems and found a number of things which were just not acceptable.

[Baldwin]: We did have one what I call minor incident in terms of our spam aspect of our firewalls so we did have one two-day period when our e-mails were overwhelmed with offers to do all kinds of different things. But there was no other incident and that by the way sort of burned out our firewall and we had to do some emergency preventative things on that. But it was nothing in terms of a data security external intrusion. It was revaluation.

[Carr]: We did learn that there was an unnecessary linkage between our payroll business and our card processing business that folks who were looking at payroll data were able to also look at card data and that was something that hadn't been planned on and we were surprised to learn and that caused us to invest some money to fix that right away as well. [Emphasis added.]

35. On or about March 10, 2008, Defendants caused Heartland to file its Annual Report with the SEC on Form 10-K. The Company's 10-K was signed by each of the Defendants

and stated, in relevant part:

> In 2007, in addition to the above-focused marketing efforts, we continued to enhance the visibility of The Merchant Bill of Rights, an advocacy initiative that educates business owners about the complexities and costs of card acceptance. ***In launching and endorsing The Merchant Bill of Rights in 2006, we committed to supporting full disclosure regarding pricing and the existence of any transaction middlemen, and for provision of dedicated customer support and high levels of security and fraud monitoring.*** This initiative has been very well received in the merchant community, and many organizations have endorsed its principles. We believe we are uniquely positioned to commit to such high customer service standards, and that our focus on this approach will continue fostering success at establishing a payment processing brand that is not easily duplicated by competitors using indirect sales models, or who do not match our focus.
>
> * * *
>
> **Network Security**
>
> In the course of our operations, we compile and maintain a large database of information relating to our merchants and their transactions. We place significant emphasis on maintaining a high level of security in order to protect the information of our merchants and their customers. We maintain current updates of network and operating system security releases and virus definitions, and have engaged a third party to regularly test our systems for vulnerability to unauthorized access. Further, we encrypt the cardholder numbers that are stored in our databases using triple-DES protocols, which represent the highest commercially available standard for encryption.
>
> ***Our internal network configuration provides multiple layers of security to isolate our databases from unauthorized access and implements detailed security rules to limit access to all critical systems.*** In response to potential security problems with payment processors' systems, Visa and MasterCard have implemented new audit procedures to highlight and repair any security weaknesses in payment processors' systems. In November 2003, we were certified by Visa as having successfully completed their Cardholder Information Security Program (CISP) review of our payment processing and Internet-based reporting systems. In 2004, the Visa CISP requirements were combined with security guidelines of the other card networks into a comprehensive Payment Card Initiative Data Security Standard (PCI-DSS). We have maintained our compliance to this standard and received recent confirmation of compliance to the standard in February 2007.
>
> Visa, Star, NYCE and other debit card networks have established security guidelines for PIN-based debit transaction processing that is based upon ANSI standards that are published as the "ASC X9 TG-3 PIN Security Compliance Guideline." We have regularly scheduled Security Review of our Key Management Procedures against this standard that is performed by an external auditor.
>
> We also have engaged external auditors to perform an annual SAS-70 review and publish our "Report on Controls Placed in Operation and Tests of Operating

Effectiveness." In addition, we have undertaken an independent Cyber-Risk Assessment.

* * *

Our systems and our third-party providers' systems may fail due to factors beyond our control, which could interrupt our service, cause us to lose business and increase our costs.

We depend on the efficient and uninterrupted operation of our computer network systems, software, data center and telecommunications networks, as well as the systems of third parties. Our systems and operations or those of our third-party providers could be exposed to damage or interruption from, among other things, fire, natural disaster, power loss, telecommunications failure, unauthorized entry and computer viruses. Our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur. Defects in our systems or those of third parties, errors or delays in the processing of payment transactions, telecommunications failures or other difficulties could result in:

• loss of revenues;

• loss of merchants, although our contracts with merchants do not expressly provide a right to terminate for business interruptions;

• loss of merchant and cardholder data;

• harm to our business or reputation;

• exposure to fraud losses or other liabilities;

• negative publicity;

• additional operating and development costs; and/or

• diversion of technical and other resources.

Unauthorized disclosure of merchant and cardholder data, whether through breach of our computer systems or otherwise, could expose us to liability and protracted and costly litigation. We collect and store sensitive data about merchants, including names, addresses, social security numbers, driver's license numbers and checking account numbers. In addition, we maintain a database of cardholder data relating to specific transactions, including bank card numbers, in order to process the transactions and for fraud prevention. Any significant incidents of loss of cardholder data by us or our merchants could result in significant fines and sanctions by Visa, MasterCard or governmental bodies, which could have a material adverse effect upon our financial position and/or operations. In addition, a significant breach could result in our being prohibited from processing transactions for Visa and MasterCard.

Our computer systems could be penetrated by hackers and our encryption of data may not prevent unauthorized use. In this event, we may be subject to liability, including claims for unauthorized purchases with misappropriated bank card information, impersonation or other similar fraud claims. We could also be

> subject to liability for claims relating to misuse of personal information, such as unauthorized marketing purposes.
>
> These claims also could result in protracted and costly litigation. In addition, we could be subject to penalties or sanctions from the Visa and MasterCard networks. Although we generally require that our agreements with our service providers who have access to merchant and customer data include confidentiality obligations that restrict these parties from using or disclosing any customer or merchant data except as necessary to perform their services under the applicable agreements, we cannot assure you that these contractual measures will prevent the unauthorized use or disclosure of data. In addition, our agreements with financial institutions require us to take certain protective measures to ensure the confidentiality of merchant and consumer data. Any failure to adequately enforce these protective measures could result in protracted and costly litigation.
>
> * * *
>
> Contingencies—The Company collects and stores sensitive data about its merchant customers and bank cardholders. If the Company's network security is breached or sensitive merchant or cardholder data is misappropriated, the Company could be exposed to assessments, fines or litigation costs.

36. On or about May 9, 2008, Defendants caused Heartland to file its Quarterly Report with the SEC on Form 10-Q. The Company's 10-Q was signed by defendants Carr and Baldwin, and stated, in relevant part:

> Contingencies—The Company collects and stores sensitive data about its merchant customers and bank cardholders. If the Company's network security is breached or sensitive merchant or cardholder data is misappropriated, the Company could be exposed to assessments, fines or litigation costs.

37. On August 8, 2008, Defendants caused Heartland to file its Quarterly Report with the SEC on Form 10-Q. The Company's 10-Q was signed by defendants Carr and Baldwin and stated, in relevant part:

> Contingencies—The Company collects and stores sensitive data about its merchant customers and bank cardholders. If the Company's network security is breached or sensitive merchant or cardholder data is misappropriated, the Company could be exposed to assessments, fines or litigation costs.

38. On November 4, 2008, Defendants caused the Company to hold an earnings conference call with investors and financial analysts. During the call defendant Carr stated, in pertinent part:

> [Carr]: We also recognize the need to move beyond the lowest common denominator of data security. Currently the PCI DSS standards. We believe it is imperative to move to a higher standard for processing secure transactions. One which we have the ability to implement without waiting for the payments infrastructure to change. We believe that standard to be -- we believe that standard to be true end-to-end encryption and we are committed to launching this new standard in the fourth quarter '09 or early 2010 with several forward-looking clients and industry partners. We believe that the payment world is at risk relying on virus protection software to protect us from determined criminal organizations. The development of the new Discover and American Express products is also progressing. We expect to be boarding new American Express installs by January 1, with Discover to follow in the first half of next year.
>
> * * *
>
> [Analyst]: Good morning, guys. Congratulations on a good quarter. Bob, just wondering about large customers. You have talked a while ago about the sales force going after large merchants. Just wanted to see if there's been any success in that area and how you perceive that opportunity at this point?
>
> [Carr]: We think that's a great opportunity. It's been very interesting talking to the large customers that we acquired with Network Services. We're a one-stop shop in the fact that we can do front end, back end, and now gift and loyalty. Big merchants like that, so that everything is integrated into one. I think we're going to be a significant player in the years coming ahead. There's not going to be anything coming down in the next few months that I know about. It's going to shock the world, but I think we're going to be able to add a lot of value to many large merchants, and we can do it in a way that is profitable because of our integrated platforms. I think you are going to see a lot of activity there. I also mentioned security. Security is a major driver of the interests of the -- not just the payment departments of large companies, but of the corporate risk officers who are very concerned about the risks of the brand in the event of a TJ Maxx or a Hannifer type problem, and the current platforms out there are not really, in my view, and in the view of a lot of the large merchants I talk to, they're not really adequate to meet the -- to counter the criminal organizations that are hacking through in various ways. I think there's a lot of play going forward. I think the world is going to change a lot over the next few years with large merchants.

39. On November 7, 2008, Defendants caused Heartland to file its Quarterly Report with the SEC on Form 10-Q. The Company's 10-Q was signed by defendants Carr and Baldwin, and stated, in relevant part:

> Contingencies—The Company collects and stores sensitive data about its merchant customers and bank cardholders. If the Company's network security is breached or sensitive merchant or cardholder data is misappropriated, the Company could be exposed to assessments, fines or litigation costs.

40. The statements contained in above were materially false and misleading when made because defendants failed to disclose or indicate the following: (1) that the Company was

in imminent danger of having the security of its processing system breached; (2) that Defendants had not taken the proper steps to secure the Company's systems; (3) that further, it was likely that the Company would not be aware such a breach occurred until weeks or months later; (4) that Defendants had been notified of a potential breach in the Company's security system; (5) that as a result, the Company would face significant costs related to, among other things, liability and the implementation of proper measures; and (6) that the Company lacked adequate internal controls.

THE TRUTH BEGINS TO EMERGE

41. On January 20, 2009, Defendants caused the Company to issue a press release entitled "Heartland Payment Systems Uncovers Malicious Software In Its Processing System." Therein, Defendants stated, in relevant part:

> Payments processor Heartland Payment Systems has learned it was the victim of a security breach within its processing system in 2008. Heartland believes the intrusion is contained. "We found evidence of an intrusion last week and immediately notified federal law enforcement officials as well as the card brands," said Robert H.B. Baldwin, Jr., Heartland's president and chief financial officer. "We understand that this incident may be the result of a widespread global cyber fraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice."
>
> * * *
>
> After being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, Heartland enlisted the help of several forensic auditors to conduct a thorough investigation into the matter. Last week, the investigation uncovered malicious software that compromised data that crossed Heartland's network.
>
> Heartland immediately took a number of steps to further secure its systems. In addition, Heartland will implement a next generation program designed to flag network anomalies in real time and enable law enforcement to expeditiously apprehend cyber criminals.

42. In response to this news, the Company's shares fell $1.26 per share, or 8.16 percent, to close on January 20, 2009 at $14.18 per share.

43. On January 22, 2009, *Bloomberg* published an article entitled "Heartland Payment

Breach May Trigger More Security Requirements." The article, in relevant part, stated:

> A computer break-in at Heartland Payment Systems Inc., the bank-card payment processor for 250,000 U.S. businesses, may prompt credit-card issuers to step up security before approving payments, analysts said. "There have to be extra security precautions put into place," said Curtis Arnold, chief executive officer of CardRatings.com, a Web site that reviews credit cards. The incident could involve 100 million accounts, Gartner Inc. analyst Avivah Litan said, citing sources in the banking industry. That would be twice the size of a 2007 attack on TJX Cos., owner of the T.J. Maxx and Marshalls discount chains, when hackers stole 45.7 million credit- and debit-card numbers, the largest such theft on record. "Fundamentally, the bad guys are very, very good," Heartland Chief Financial Officer Robert Baldwin said yesterday in an interview. "We're deeply disappointed." One potential security move may follow the lead of Citigroup Inc.'s Virtual Account Numbers program, which generates a unique number with limited uses for online purchases, Arnold said. Verified by Visa, which confirms the online shopper's identity with an extra Heartlandion, is another "under-utilized" program, he said.
>
> "Malicious software that compromised data that crossed Heartland's network" was found in the processing system last week, the Princeton, New Jersey-based company said in a statement Jan. 20. The breach occurred sometime in 2008, the company said.
>
> **Totally Speculative**
>
> Heartland doesn't know how many accounts were affected and any estimate is "totally speculative," Baldwin said.
>
> Heartland fell 7 cents to $14.11 yesterday in New York Stock Exchange composite trading. The shares lost 34 percent in the 12 months before today. Heartland set up a Web site to provide consumers with information about the investigation at http://www.2008breach.com.
>
> The company discovered the breach after Visa Inc. and MasterCard Inc. warned of suspicious activity surrounding processed card transactions, Heartland said, without providing details. The attack apparently came through the Internet, not someone inside Heartland, Baldwin said.
>
> "If you're a criminal and attack that data from offshore, you reduce the risk of getting caught," said Mark Bower, director of information protection solutions for Palo Alto, California-based Voltage Security Inc., which provides encryption services. "It's more lucrative than the traditional bank robbing."
>
> **Consumer Liability**
>
> Heartland, which has insurance to cover a portion of the costs of the breach, doesn't know how much of a charge the company will take because of the theft, Baldwin said. If a card is used fraudulently, a consumer is liable for a maximum of $50.

> "This is obviously a huge liability for Heartland," said David Robertson, publisher of the Nilson Report, which tracks the creditcard industry. "The Heartlandion is how many data breaches does it take for the industry to change?"
>
> TJX agreed to pay as much as $24 million to issuers of MasterCards and $40.9 million to Visa issuers to cover fraud losses from its computer breach. Credit and debit card security should be more like that used by banks, said Eddie Woodruff, chief marketing officer at Lexington, Kentucky-based Forcht Bank, which reissued 8,500 debit cards because of the Heartland breach. To provide online security, banks ask Heartlandions that only the proper user could answer, such as the name of a school he or she attended.
>
> "The online banking system has gone to multi-layer identification," Woodruff said. "We will see that in debit cards as well."

44. On this news, the Company's shares fell an additional $5.93 per share, or 42.03 percent, to close on January 22, 2009 at $8.18 per share, on unusually heavy trading volume.

45. Then, on February 24, 2009, Defendants caused the Company to issue a press release entitled "Heartland Payment Systems Reports Fourth Quarter Earnings of $0.21 Per Diluted Share." Therein, Defendants, stated in relevant part:

> Heartland Payment Systems, Inc. (NYSE: HPY), a leading provider of credit/debit/prepaid card processing, payroll, check management and payment services, today announced quarterly net income of $8.0 million and fully diluted earnings per share of $0.21 for the three months ended December 31, 2008. Earnings in the current quarter were up compared to net income of $6.8 million, or $0.17 per fully diluted share in the fourth quarter of 2007. Earnings in the year ago quarter include an aggregate $2.9 million in pre-tax charges (approximately $0.05 per share) to write off an investment and to recognize costs associated with the opening and relocation to our new service center.
>
> * * *
>
> Mr. Carr continued, "Heartland has been built on a foundation of fair dealings, pricing transparency and merchant advocacy. Since our formation almost 12 years ago, our commitment to these principles has enabled us to grow into one of the largest companies in our industry. As the victim of a malicious system breach, we are highly focused on once again moving our industry forward, now taking the lead in strengthening the safety and security of information throughout the entire payments processing network. Heartland is committed to aggressively pursuing its efforts for the development and industry-wide implementation of end-to-end encryption technology- which if successfully developed and implemented will be designed to protect data at rest as well as data in motion—as an improved and safer standard of payments security.
>
> ***"Clearly our biggest challenge in 2009 will arise from the system breach we suffered. There are two main components to the challenge we face: addressing claims that cardholders, card issuers, the Brands, regulators, and others have***

asserted, or may assert, against us arising out of the breach and managing the potential impact of the breach on the day-to-day operations of our business. With regard to the first challenge, we intend to vigorously defend any such claims and we believe we have meritorious defenses to those claims that have been asserted to date. At this time we do not have information that would enable us to reasonably estimate the amount of losses we might incur in connection with such claims. As to the second challenge, our sales and service teams have responded tremendously, and early indications of client response are positive: in the weeks since our announcement of the breach, we have installed more margin, and have a bit less merchant attrition, than in the same period in 2008.

While it is too early to tell, and we will certainly face challenges from macro economic conditions confronting our customers, at this point we believe that our expanded product breadth, reputation for superior customer service, candor, and no arbitrary rate increases, should allow us to grow our card processing merchants, payroll clients and check management clients in 2009. I am very proud of our Heartland employees, who are aggressively reaching out to strengthen our relationships and maintain the trust and confidence of the merchant community."

FULL YEAR 2008 RESULTS:

For the full year 2008, net income was $41.8 million or $1.08 per fully diluted share, increases of 16.6% and 20.0%, respectively, from 2007 reported amounts of $35.9 million and $0.90, respectively. The 2007 reported net income included an aggregate $2.9 million in pre-tax charges (approximately $0.05 per share) to write off an investment and to recognize costs associated with the opening and relocation of our new service center. Net Revenues for 2008 were $383.7 million, up 30.2% compared to 2007. Excluding Network Services, net revenue was up 15.3% to $340.0 million.

FULL YEAR 2009 GUIDANCE:

Current economic conditions, the breach, and the financial climate are likely to influence same store sales growth and new merchant signings, necessarily adding conservatism to our guidance. For the year, we expect net revenue (total revenues less interchange, dues and assessments) to grow by 12—16%, to between $430 and $445 million, with 7 – 11% of that growth organic. For the year, earnings per share are expected to be $1.15—$1.22. The Company's guidance for 2009 does not include any estimates for potential losses, costs and expenses arising from the previously announced security breach, including exposure to credit and debit card companies and banks, exposure to various legal proceedings that are pending, or may arise, and related fees and expenses, and other potential liabilities, costs and expenses. Neither the costs nor the potential losses are estimable at this point, and further the potential losses are not currently deemed probable.

DIVIDEND:

The Company also announced that, in light of the difficulties in the financial markets, the Board of Directors believes it is prudent to maximize the Company's financial resources and liquidity.

> Consequently, ***the Board of Directors has established a new dividend rate and declared a quarterly dividend of $0.025 per common share,*** which is payable March 16, 2009 to shareholders of record on March 9, 2009.

46. Also on February 24, 2009, Defendants caused the Company to hold an earnings conference call with analysts and investors. During the call, defendants Carr and Baldwin stated, in relevant part:

> [Carr]: While it is too early to tell for sure, and ***we will certainly face challenges from the macroeconomic conditions confronting our customers and related to our system breach,*** based on the results we have seen so far for this year, we expect our success in the market to continue in 2009. At the end of 2008, our sales organization was up 4% from a year ago to 1,166 relationship managers and our team of account managers who install new merchants and manage ongoing relationships has grown 22% to 29%.
>
> * * *
>
> On January 20, of '09, we announced the discovery of malware in our payment systems environment, apparently resulting from a criminal breach. Potentially exposed through this breach of the payment environment were card numbers, expiration dates and their data from the cards' magnetic stripe. In a small percentage of cases, the card holder name also appears to have been exposed.
>
> However, the card holder information we processed does not include addresses or Social Security numbers. We also believe that no unencrypted pin data was captured and we believe the breach has been contained and did not extend beyond '08.
>
> ***In late October, we were alerted by Visa of suspicious activity surrounding certain accounts that appeared to certain issuers to have been subjected to fraudulent activity shortly after they were used to make legitimate transactions that were processed by Heartland.*** Our IT team worked with the brand to try to match the suspicious transactions with our processing activities. And we engaged forensic auditors to evaluate different parts of our processing platform to investigate whether there was a potential problem. Ultimately, one of those firms provided our team with information that led us to discover malware output files on January 12 and on January 13, led us to the discovery of malicious software that apparently had created these files.
>
> These malicious software programs were able to read and collect data in unencrypted form as it was in motion, which is when it was being sent to the switches that transmit data to the card brands during the transaction authorization process. The intruder potentially may have been able to ex-filtrate from the network some of the data collected by means of the malware. Keep in mind that Heartland passed its PCI certification last April and assessors are currently on-site for the 2009 certification, which we are targeting to complete by the end of April. In that regard, throughout the potential period of the breach, Heartland did have antivirus software installed on its payment processing network.

> ***The length of time that the malicious software was on the servers is not clear, though at this time, we believe it ceased being active during 2008.*** Further, it seems clear that the malware was not active at all times during this period, and it was probably not capturing information from 100% of transactions flowing through the system even when active or exporting all of the captured information to the criminals. ***For this reason, it is simply not possible at this time to determine accurately the number of card accounts that had information placed at risk of compromise during the breach, or to what extent any such information placed at risk was in fact compromised.***
>
> * * *
>
> [Baldwin]: To date, we have had several lawsuits filed against us and we expect that additional lawsuits will be filed. ***We are also the subject of several governmental investigations and inquiries, including an informal inquiry by the SEC and a related investigation by the Department of Justice, an inquiry by the OCC, and an inquiry by the FTC, and we may, in the future, be subject to other governmental inquiries and investigations.*** We intend to vigorously defend any claims asserted against us and we believe we have meritorious defenses to the claims asserted against us to date.
>
> At this time, we do not have information that would enable us to reasonably estimate the amount of any losses we might incur by reason of such claims, and such losses are not currently deemed probable. ***We recognize, however, that we may incur losses in connection with the breach and that such losses could be material and could have a material adverse impact on our results of operations and financial condition.***

47. On this news, the Company's shares fell an additional $2.31 per share, or 30.2 percent, to close on February 24, 2009 at $5.34 per share, on unusually heavy trading volume.

DERIVATIVE AND DEMAND ALLEGATIONS

48. Plaintiff brings this action derivatively in the right and for the benefit of Heartland to redress the breaches of fiduciary duty and other violations of law by Defendants.

49. Plaintiff will adequately and fairly represent the interests of Heartland and its shareholders in enforcing and prosecuting its rights.

50. The Board currently consists of the following seven (7) individuals: defendants Carr, Hollin, Niehaus, Palmer, Raymond, Ostro, and Vague. Plaintiff has not made any demand on the present Board to institute this action because such a demand would be a futile, wasteful and useless act, for the following reasons:

a. During the Relevant Period, defendants Palmer, Raymond, and Ostro served as members of the Audit Committee. Pursuant to the Company's Audit Committee Charter, members of the Audit Committee are responsible for, *inter alia*, monitoring the Company's systems of internal controls, monitoring the integrity of the Company's financial statements and earnings press releases, and monitoring compliance with ethical policies and legal and regulatory requirements. Defendants Palmer, Raymond, and Ostro breached their fiduciary duties of due care, loyalty, and good faith, because the Audit Committee, *inter alia*, allowed or permitted false and misleading statements to be disseminated in the Company's SEC filings and other disclosures and failed to ensure that adequate internal controls were in place. Therefore, defendants Palmer, Raymond, and Ostro face a substantial likelihood of liability for their breach of fiduciary duties and any demand upon them is futile; and

b. The principal professional occupation of defendant Carr is his employment with Heartland as its CEO, pursuant to which he has received and continues to receive substantial monetary compensation and other benefits. Thus, defendant Carr lacks independence, rendering him incapable of impartially considering a demand to commence and vigorously prosecute this action.

c. During the Relevant Period, pursuant to the Company's Code of Business Conduct and Ethics for Directors, Officers, and Employees, each member of the Board was required, *inter alia*, to provide "stockholders and investors with full, fair, accurate, [and] timely" disclosures. Defendants Carr, Hollin, Niehaus, Palmer, Raymond, Ostro, and Vague breached their fiduciary duties of due care, loyalty, and good faith, because, *inter alia*, they issued, allowed, or permitted false and misleading statements which were disseminated in the Company's SEC filings and other public disclosures. Accordingly, the entire Board faces a substantial likelihood of liability for their breach of fiduciary duties and any demand upon the Board is futile.

COUNT I
AGAINST ALL DEFENDANTS FOR BREACH OF FIDUCIARY DUTY FOR DISSEMINATING FALSE AND MISLEADING INFORMATION

51. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

52. As alleged in detail herein, each of the Defendants (and particularly the Audit Committee Defendants) had a duty to ensure that Heartland disseminated accurate, truthful and complete information to its shareholders.

53. Defendants violated their fiduciary duties of care, loyalty, and good faith by

causing or allowing the Company to disseminate to Heartland shareholders materially misleading and inaccurate information through, *inter alia*, SEC filings and other public statements and disclosures as detailed herein. These actions could not have been a good faith exercise of prudent business judgment.

54. As a direct and proximate result of Defendants' foregoing breaches of fiduciary duties, the Company has suffered significant damages, as alleged herein.

COUNT II
AGAINST ALL DEFENDANTS FOR BREACH OF FIDUCIARY DUTIES FOR FAILING TO PROPERLY OVERSEE AND MANAGE THE COMPANY

55. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

56. Defendants owed and owe Heartland fiduciary obligations. By reason of their fiduciary relationships, Defendants specifically owed and owe Heartland the highest obligation of good faith, fair dealing, loyalty and due care.

57. Defendants, and each of them, violated and breached their fiduciary duties of care, loyalty, reasonable inquiry, oversight, good faith and supervision.

58. As a direct and proximate result of Defendants' failure to perform their fiduciary obligations, Heartland has sustained significant damages, not only monetarily, but also to its corporate image and goodwill.

59. As a result of the misconduct alleged herein, Defendants are liable to the Company.

60. Plaintiff, on behalf of Heartland, has no adequate remedy at law.

COUNT III
AGAINST ALL DEFENDANTS FOR BREACH OF FIDUCIARY DUTIES FOR FAILING TO MAINTAIN INTERNAL CONTROLS

61. Plaintiff incorporates by reference all preceding and subsequent paragraphs as if

fully set forth herein.

62. As alleged herein, each of the Defendants (and particularly, the Audit Committee Defendants) had a fiduciary duty to, among other things, exercise good faith to ensure that the Company had adequate systems of internal controls in place, and, when put on notice of problems with the Company's business practices and operations, exercise good faith in taking appropriate action to correct the misconduct and prevent its recurrence.

63. Defendants willfully ignored the obvious and pervasive problems with Heartland's internal controls practices and procedures and failed to make a good faith effort to correct the problems or prevent their recurrence.

64. As a direct and proximate result of the Defendants' foregoing breaches of fiduciary duties, the Company has sustained damages.

COUNT IV
AGAINST ALL DEFENDANTS FOR UNJUST ENRICHMENT

65. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

66. By their wrongful acts and omissions, the Defendants were unjustly enriched at the expense of and to the detriment of Heartland.

67. Plaintiff, as a shareholder and representative of Heartland, seeks restitution from these Defendants, and each of them, and seeks an order of this Court disgorging all profits, benefits and other compensation obtained by these Defendants, and each of them, from their wrongful conduct and fiduciary breaches.

COUNT V
AGAINST ALL DEFENDANTS FOR ABUSE OF CONTROL

68. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

69. Defendants' misconduct alleged herein constituted an abuse of their ability to control and influence Heartland, for which they are legally responsible. In particular, Defendants abused their positions of authority by causing or allowing Heartland to misrepresent material facts regarding its financial position and business prospects.

70. As a direct and proximate result of Defendants' abuse of control, Heartland has sustained significant damages.

71. As a result of the misconduct alleged herein, Defendants are liable to the Company.

72. Plaintiff, on behalf of Heartland, has no adequate remedy at law.

COUNT VI
AGAINST ALL DEFENDANTS FOR GROSS MISMANAGEMENT

73. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

74. Defendants had a duty to Heartland and its shareholders to prudently supervise, manage and control the operations, business and internal financial accounting and disclosure controls of Heartland.

75. Defendants, by their actions and by engaging in the wrongdoing described herein, abandoned and abdicated their responsibilities and duties with regard to prudently managing the businesses of Heartland in a manner consistent with the duties imposed upon them by law. By committing the misconduct alleged herein, Defendants breached their duties of due care, diligence and candor in the management and administration of Heartland's affairs and in the use and preservation of Heartland's assets.

76. During the course of the discharge of their duties, Defendants knew or recklessly disregarded the unreasonable risks and losses associated with their misconduct, yet Defendants

caused Heartland to engage in the scheme complained of herein which they knew had an unreasonable risk of damage to Heartland, thus breaching their duties to the Company. As a result, Defendants grossly mismanaged Heartland.

COUNT VII
AGAINST ALL DEFENDANTS FOR WASTE OF CORPORATE ASSETS

77. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

78. As a result of the misconduct described above, and by failing to properly consider the interests of the Company and its public shareholders, Defendants have caused Heartland to incur (and Heartland may continue to incur) significant legal liability and/or legal costs to defend itself as a result of Defendants' unlawful actions.

79. As a result of this waste of corporate assets, Defendants are liable to the Company.

80. Plaintiff, on behalf of Heartland, has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment as follows:

A. Against all Defendants and in favor of the Company for the amount of damages sustained by the Company as a result of Defendants' breaches of fiduciary duties;

B. Directing Heartland to take all necessary actions to reform and improve its corporate governance and internal procedures to comply with applicable laws and to protect the Company and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote resolutions for amendments to the Company's By-Laws or Articles of Incorporation and taking such other action as may be necessary to place before shareholders for a vote a proposal to strengthen the Board's

supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board

C. Awarding to Heartland restitution from Defendants, and each of them, and ordering disgorgement of all profits, benefits and other compensation obtained by the Defendants;

D. Awarding to Plaintiff the costs and disbursements of the action, including reasonable attorneys' fees, accountants' and experts' fees, costs, and expenses; and

E. Granting such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff demands a trial by jury.

Dated: July 14, 2009

BRODSKY & SMITH, LLC

By:*s/ Evan J. Smith, Esquire*
Evan J. Smith, Esquire
esmith@brodsky-smith.com
1040 Kings Highway N., Suite 601
Cherry Hill, NJ 08034
Telephone: (856) 795-7250
Facsimile: (856) 795-1799

THE WEISER LAW FIRM, P.C.
Robert B. Weiser, Esquire
Brett D. Stecker, Esquire
Jeffrey J. Ciarlanto, Esquire
121 N. Wayne Avenue, Suite 100
Wayne, PA 19087
Telephone: (610) 225-2677
Facsimile: (610) 225-2678

Counsel for Plaintiff

HEARTLAND PAYMENT SYSTEMS, INC. VERIFICATION

I, Eric Kirkham, hereby verify that I am familiar with the allegations in the Complaint, and that I have authorized the filing of the Complaint, and that the foregoing is true and correct to the best of my knowledge, information, and belief.

Date: 7/10/09

Eric Kirkham